PERMUTATION POLYTOPES AND INDECOMPOSABLE ELEMENTS IN PERMUTATION GROUPS

ROBERT GURALNICK AND DAVID PERKINSON

ABSTRACT. Each group G of $n \times n$ permutation matrices has a corresponding permutation polytope, $P(G) := \mathrm{conv}(G) \subset \mathbb{R}^{n\times n}$. We relate the structure of $P(G)$ to the transitivity of G. In particular, we show that if G has t nontrivial orbits, then $\min\{2t, \lfloor n/2 \rfloor\}$ is a sharp upper bound on the diameter of the graph of $P(G)$. We also show that $P(G)$ achieves its maximal dimension of $(n-1)^2$ precisely when G is 2-transitive. We then extend the results of Pak [22] on mixing times for a random walk on $P(G)$. Our work depends on a new result for permutation groups involving writing permutations as products of indecomposable permutations.

1. INTRODUCTION

Let G be a subgroup of S_n, the symmetric group on $\{1, 2, \ldots, n\}$. Via the usual representation of G as a group of $n \times n$ permutation matrices, each element of G may be considered as an element of $\mathbb{R}^{n^2}$. The convex hull in $\mathbb{R}^{n^2}$ of the elements of G is $P(G)$, the *permutation polytope* associated with G. Permutation polytopes and their linear projections have been studied extensively due to their connection to problems in combinatorial optimization [5], [6], [20], [24]. The most well-known example is the case where $G = S_n$ with corresponding permutation polytope called the n-th *Birkhoff polytope* or the n-th *assignment polytope* [9], [10], [24]. Even here there are open problems [22]; for instance, its volume is known only up to $n = 10$ [7]. Some newer applications of permutation polytopes are to group resolutions [13] and communications networks [17], [23].

The main concern of this paper is to establish links between (algebraic) properties of an arbitrary permutation group G and (geometric) properties of its corresponding permutation polytope $P(G)$. We are

Date: November 16, 2005.

The first author acknowledges support from the NSF grant DMS 0140578. We thank D. Goldstein for his comments on earlier drafts. We also thank J. Buhler and I. Pak for their input. Finally, we thank the referees for their comments.

especially interested in ways in which the transitivity of G is reflected in its polytope. First, Theorem 2.1, shows that every element of a transitive permutation group can be written as a product of at most two so-called indecomposable elements (see §2 for definitions). The geometric consequence is Corollary 3.7: if G has t non-trivial orbits, then the diameter of $P(G)$, i.e., the diameter of the edge graph of $P(G)$, is bounded by $\min\{2t, \lfloor n/2 \rfloor\}$. Thus, if G is transitive, the diameter of $P(G)$ is at most 2. This generalizes previous work establishing the diameters of the Birkhoff polytopes [4], [25] and the diameters of the polytopes corresponding to the groups of even permutations [11]. In the language of Babai et al. [3], we have bounded the diameter of *the group* G with respect to the set of generators consisting of its indecomposable elements.

Corollary 3.7 relies on Theorem 3.5 characterizing the smallest face of a permutation polytope containing two prescribed vertices (group elements) in terms of their cycle structure. In particular, we characterize the edges of a permutation polytope, as previously known for the Birkhoff polytopes [21] and for the polytopes corresponding to the groups of even permutations [11]. The special case $G = S_n$ in Theorem 3.5 is Proposition 2.1 in [8].

The other main result concerning transitivity is Corollary 3.4, showing that the dimension of $P(G)$ is bounded by $(n-1)^2$ with equality if and only if G is 2-transitive. The dimension of the n-th Birkhoff polytope is known to equal the maximum value, $(n-1)^2$, by an easy calculation in linear algebra. With more work, one may similarly show that the maximum dimension is achieved when G is the collection of all even permutations and $n \geq 4$ [11]. Corollary 3.4 generalizes these results and provides a conceptual explanation.

In the final section of the paper, we generalize the results of [22] about the mixing time of random walks on these polytopes. This says that random products of indecomposable elements tend to the uniform distribution very quickly for G primitive (Pak [22] handles the case of the Birkhoff polytope).

The results in this paper stem from systematic experimentation using the computer programs GAP [14] for group theory and Polymake [15] for polytopes.

2. Permutation Groups

Let G be a permutation group acting faithfully on a (finite) set X. We say $g \in G$ is indecomposable if $g \neq xy$ where x, y are nontrivial elements of G and $M(x) \cap M(y)$ is empty, where $M(x)$ is the *support* of x: the set of points of X moved by x. Let $F(x)$ be the set of fixed points of x and $f(x) = |F(x)|$.

We shall prove:

Theorem 2.1. *Let G be transitive on X. Then every element of G is a product of at most 2 indecomposable elements.*

In fact, for inductive purposes, it is better to prove a slightly stronger result:

Theorem 2.2. *Let G be transitive on X. Then every element of G is a product of two elements, each indecomposable and at least one fixed point free.*

We will prove this result in the next few subsections. We first show that it suffices to assume that G acts primitively on the set X (i.e. preserves no nontrivial partition of X).

We then show that the result holds when the group is primitive and not almost simple (recall a group is almost simple if it has a unique minimal normal subgroup that is a nonabelian simple group).

Finally, we show that in the almost simple case, aside from the case that G contains $\mathrm{Alt}(X)$, every element is indecomposable (whence the result follows since fixed point free elements in a finite transitive permutation group always exist). The result in the case $G = \mathrm{Alt}(X)$ or $\mathrm{Sym}(X)$ is elementary.

We do have to invoke the classification of finite simple groups to handle the case that G is almost simple. The key result we use is the classification of primitive permutation groups containing a nontrivial element with $f(x) \geq |X|/2$.

We first point out some easy consequences of Theorem 2.2 using the following lemma.

Lemma 2.3. *Suppose that $X = Y \cup Z$ is a finite G-set with Y and Z invariant under G. Let N be the normal subgroup of G acting trivially on Y. If every element of G/N acting on Y can be written as a product of r indecomposables and every element of N can be written as a product of s indecomposables, then every element of G is a product of $r + s$ indecomposables.*

Proof. If $g \in G$, let g_Y denote g considered as permutation on Y.

We claim that if $g \in G$ and g_Y is indecomposable, then gn is indecomposable for some $n \in N$.

Proof of Claim: If g is indecomposable, we are done. If not, write $g = hu$ where $M(h) \cap M(u)$ is empty and h is not in N. Since g_Y is indecomposable, $h_Y = g_Y$ and $u \in N$. Thus, $h \in gN$ is indecomposable.

The claim implies that we can write $g \in G$ as a product of r indecomposables (or fewer) times an element of N. By assumption, the element in N can be written as a product of s indecomposables (in N and thus also in G). □

Corollary 2.4. *If $G \leq S_n$, then every element of G can be written as a product of $2t$ indecomposables where t is the number of nontrivial orbits of G.*

Corollary 2.5. *If $G \leq S_n$, then every element of G can be written as a product of $\lfloor n/2 \rfloor$ indecomposables.*

Proof. By induction and the lemma above, it suffices to consider the case that G is transitive. By the theorem, the result holds for $n \geq 4$. Inspection shows that for $n \leq 3$, every nontrivial element is indecomposable. □

2.1. **Reduction to the Primitive Case.** Let G be a group acting faithfully and transitively on the finite set X. Let $n = |X| > 1$.

Lemma 2.6. *Let $Y := \{X_1, \dots, X_m\}$ be a nontrivial G-invariant partition of X. Let N be the normal subgroup of G preserving each X_i. Let $g \in G$.*

1. *If gN is fixed point free and indecomposable on Y, then every element in gN is fixed point free and indecomposable on X.*
2. *If gN is indecomposable on Y, then there is some element in gN that is indecomposable on X.*

Proof. We prove both statements simultaneously. Reordering if necessary, we may assume that g moves the sets $X_1, \dots, X_e$ and fixes the other X_i. Assume also that gN is indecomposable on Y.

Suppose that $g = xy$ where $M(x) \cap M(y)$ is empty. Then $gN = xNyN$ and xN and yN cannot move a common X_i. Since gN is indecomposable, we may assume that $gN = xN$ and $yN = N$. Thus, $x \in gN$ and the second statement holds.

Moreover, since x and y share no moved points, y must be trivial on each block moved by g. So if gN has no fixed points on Y, then $y = 1$ and $g = x$ is indecomposable. □

An immediate consequence is:

Corollary 2.7. *Suppose that (G, X) is a counterexample to Theorem 2.2 with $|X|$ minimal. Then G acts primitively on X.*

Proof. If G preserves a nontrivial partition Y on X, let N be the normal subgroup acting trivially on the partition. By the previous result,

$(G/N, Y)$ is a counterexample to Theorem 2.2, contradicting the minimality of $|X|$. □

We deal with the case that G acts primitively on X in the next two subsections.

2.2. **Primitive Groups I.** In this subsection, we assume that G is not almost simple and acts primitively (and faithfully) on the finite set X of cardinality n.

The structure of finite primitive groups is quite constrained. See [2] for a detailed description.

Recall that a transvection is a nontrivial unipotent linear transformation which is trivial on a hyperplane.

Theorem 2.8. *Assume that G contains a regular normal subgroup N. Then one of the following holds:*

(1) *Every element of G is indecomposable.*
(2) *N is an elementary abelian 2-group of order $2^a \geq 4$ and $G = NH$ where H is a subgroup of $\mathrm{GL}(a, 2) = \mathrm{Aut}(N)$ acting irreducibly on N and containing transvections.*

Moreover, G satisfies the conclusion of Theorem 2.2.

Proof. It follows by [2] that N is a direct product of isomorphic copies of a simple group L. If $g \in G$ has a fixed point, then as g-set, we can identify X with N and the fixed points of g are identified with $C_N(g)$. Unless $|L| = 2$, any proper subgroup of N has index at least 3, so for $1 \neq g$, the proportion of fixed points is at most $1/3$. Thus, $M(x) \cap M(y)$ is nonempty for any two nontrivial elements in G and so (1) holds.

So N is an elementary abelian 2-group of order 2^a. If $a = 1$, then G is cyclic of order 2 and the result hold. If $a > 1$, the argument of the previous paragraph applies and we see that $f(g) \leq n/2$ with equality if and only if g induces a transvection acting on N. Thus either (1) or (2) hold.

So it suffices to prove the last statement in the case $G = NH$ where $|N| = n = 2^a \geq 4$ and $G = NH$ with H acting irreducibly and faithfully on N and containing transvections. Note that if $x \in G$ is decomposable, then $x = uv$ where u, v are involutions fixing precisely one half the points of X. Moreover, u and v commute and the fixed point sets of u and v must be disjoint. Thus, x is a fixed point free involution.

If $a = 2$, then $G = S_4$ and the result holds by inspection. So assume that $a > 2$ and g is a fixed point free involution.

First suppose that $g \in N$. Choose $h_1, h_2 \in H$ that are noncommuting transvections (if all transvections in H commute they would generate a normal unipotent subgroup of H and this contradicts the irreducibility of H). So $h_1 h_2$ has order 3 and $\langle h_1, h_2 \rangle$ centralizes a subgroup N_0 a subgroup of index 4 in N. Let $1 \neq v \in N_0$ (this is possible since $a > 2$). Then $h := h_1 h_2 v$ has order 6 and is fixed point free (since $h^3 = v$ is). Finally, we see that $g = h(h^{-1}g)$ and $h^{-1}g$ has order a multiple of 3 and so is indecomposable.

Finally, suppose that g is a fixed point free involution not in N. Let h_1 and h_2 be noncommuting transvections in H. Choose $v_i \in N, 1 \leq i \leq 2$ so that $w_i := h_i v_i$ has order 4 (and so is fixed point free and indecomposable). Let v be a nontrivial element of N_0 (as in the previous paragraph). Set $w_3 := h_1 h_2 v$. So w_3 has order 6 and is fixed point free.

We claim that g cannot invert each of w_1, w_2 and w_3 – for if so, then g would invert each element in G/N and $\langle w_1 N, w_2 N \rangle$ is isomorphic to S_3. So choose a w_i not inverted by g. Then $g = (gw_i)w_i^{-1}$. Since gw_i does not have order 2, it is indecomposable and we have noted already that w_i is indecomposable and fixed point free.

This completes the proof. □

There are few irreducible groups containing transvections. See [19]. If G is a solvable primitive permutation group of degree n, then G does contain a regular normal subgroup. Thus, using the previous result and [19] yields:

Corollary 2.9. *If G is a primitive solvable subgroup of S_n, then one of the following holds:*

1. *Every element of G is indecomposable;*
2. *$n = 4$ and $G = S_4$; or*
3. *$n = 16$ and G has a normal regular elementary abelian subgroup N of order 16 and $G/N = 0_4^+(2)$.*

We can now handle all primitive groups other than the almost simple groups.

Theorem 2.10. *Assume that G acts faithfully and primitively on the set X of cardinality $n > 1$. Assume that G is not almost simple. Every element of G can be written as a product of two indecomposable elements, one of which is fixed point free.*

Proof. By the previous result, we may assume that G does not contain a regular normal subgroup. We may also assume that some nontrivial element of G fixes at least $n/2$ points. It follows by the structure of primitive groups [2], the previous result and [16] that G preserves a Cartesian product structure on X.

More precisely, we can write

$$X = X_1 \times \ldots \times X_m,$$

where $m > 1$, $|X_i| = e \geq 5$ and $G \leq T := S_e \wr S_m = W.S_m$ where

$$W = S_e \times \ldots \times S_e$$

acting coordinatewise on X and S_m permutes the coordinates. Furthermore, G has a unique minimal normal subgroup

$$N := L_1 \times \ldots \times L_m$$

where $L_i \cong L$ is a nonabelian simple and L_i acts on X_i and trivially on X_j for $j \neq i$.

Let W_i be the ith copy of S_e in W.

We claim that $g \in G$ is decomposable implies $g \in W_i$ for some i. It suffices to show that this is the case for T. Suppose that $x, y \in T$ are nontrivial elements and $M(x) \cap M(y)$ is empty. Suppose that x acts on an X_i and y on an X_j with $j \neq i$. Choose $a \in X_i$ moved by x and $b \in X_j$ moved by y. Then any point of X whose ith coordinate is a and jth coordinate is b is moved by x and y, a contradiction.

This shows that if x and y are both in W, then they are both in W_i for some i and so also xy. If neither x nor y is in W, then x and y each move at least $n - n/e > n/2$ points and so $M(x) \cap M(y)$ is nonempty. Finally, suppose that x is not in W and $y \in W$. Arguing as above, we see that it suffices to consider the case that x permutes the X_i transitively. Say y is nontrivial on X_1 and moves $a \in X_1$. Then x cannot fix all points of X with first coordinate a and so $M(x) \cap M(y)$ is empty.

This proves the claim.

We now complete the proof of the result.

Let $g \in G$. If g is not in W, then choose $h \in N$ with h not in $N \cap W_i = L_i$ for any i and h fixed point free (just choose $h_1 \in L_1$ fixed point free and h_2 nontrivial). Then $g = h(h^{-1}g)$ is the desired decomposition ($h^{-1}g$ is not in W and so indecomposable). If $g \in W$, we choose a similar h guaranteeing that $h^{-1}g$ is not in W_i for any i.

□

2.3. **Almost Simple Groups.** We now consider almost simple groups. So G is an almost simple group and has socle S and acts transitively on X of cardinality $n > 1$.

We first deal with the cases $G = A_n$ or S_n. Note that the lemma is just the theorem for these groups.

Lemma 2.11.
(1) *Any element of S_n can be written as a product of an n-cycle and a k-cycle for some k.*
(2) *If n is even, then every element of A_n can be written as product xy where x has exactly two orbits each of even length and y is a k-cycle or y has precisely two nontrivial orbits each of even length.*

Proof. Suppose that g has k orbits.

Let h be a k-cycle moving precisely one point in each g-orbit. Then gh is an n-cycle, whence (1) holds.

Now suppose that n is even and $g \in A_n$. If $g = 1$, the result is clear. Otherwise, write $g = xy$ where x is an n-cycle and y is a k-cycle. Necessarily k is even and the construction above shows that we can take $k < n$.

Let t be a transposition moving at least 1 point fixed by y. Then xt has precisely 2 orbits and we can pick t so that each of the orbits is even. Then ty is either a $k+1$ cycle (if t and y are not disjoint) or has two nontrivial orbits (of length 2 and k). So $g = (xt)(ty)$, whence (2) holds. □

If no element fixes at least half the points, then clearly every element is indecomposable. By [16], the only cases to consider are dealt with in the next three lemmas.

Lemma 2.12. *Let $G = A_n$ or S_n with $n \geq 5$ acting on X, the set of k-sets for some k with $1 < k < n/2$. Then every element of G is indecomposable.*

Proof. We show that for x, y nontrivial, $M(x)$ and $M(y)$ have a nonempty intersection. Let $Y = \{1, 2, \ldots, n\}$. If $x \in G$ and $j \in Y$, we write xj for the image of j under x.

First suppose that x and y move a common point in the natural representation. So we may assume that x and y each move 1. Let D be a k-set containing 1 but missing $x1$ and $y1$. Then x and y both move D.

Suppose that x and y move no common point in Y. So we may assume that x moves 1 and y moves 2. Let D be a k-set containing $1, 2$ but not containing $x1$ and $y2$. Then x and y both move D. □

Lemma 2.13. *Let $G = \mathrm{Sp}(2d, 2)$ with $d \geq 3$. Let X be the coset space G/H where $H = \mathrm{O}^-(2d, 2)$ (note that this is the set of nondegenerate hyperplanes of $-$ type in the $2d+1$ dimensional orthogonal module for G). Every element of G is indecomposable on X.*

Proof. Suppose that $M(x) \cap M(y)$ for x, y nontrivial in G. It is easy to see (cf [16]) that every nontrivial element other than a transvection moves more than $|X|/2$ elements. So we choose notation so that x is a transvection and $y \neq x$. Let $P = C_G(x)$. Then P is a maximal parabolic subgroup of G. Then y fixes each coset of H moved by x. The same is true for any P-conjugate of y and so $J := \langle y^P \rangle$ does as well. So P normalizes J. Now J is proper in G and so as G is simple and P is maximal, J is a nontrivial normal subgroup of P. The subgroup generated by x is the unique minimal normal subgroup of P and so $x \in J$. However, x certainly moves all the points of $M(x)$ and this contradiction completes the proof. □

Lemma 2.14. *Let $G^\epsilon = \mathrm{O}^\epsilon(2d, 2)$ with $d > 2$. Let X be the set of singular vectors (if $\epsilon = -$) or the set of nonsingular vectors (if $\epsilon = +$). Every element of G^ϵ is indecomposable on X.*

Proof. Let $J = \mathrm{Sp}(2d, 2)$ and Y the J-set described in the previous lemma. Note that G^ϵ is a subgroup of J and so acts on Y. If $\epsilon = +$, then $Y \cong X$ at G^+-sets. Also, G^- fixes one point of Y and the remaining orbit is isomorphic to X as a G^- set. Thus, the result follows from the previous lemma. □

The previous three lemmas together with [16] immediately yields:

Theorem 2.15. *Let B be an almost simple group acting primitively on X. Then either every element of G is indecomposable or G contains $\mathrm{Alt}(X)$.*

For almost simple groups, we can weaken the assumption of primitivity.

Theorem 2.16. *Let G be an almost simple group transitive permutation group of degree n and suppose that some element of g is decomposable. Then G is a symmetric group or alternating group of degree m for some m dividing n.*

Proof. If G is primitive on X, this follows from the previous result. Suppose that G is not primitive on X and some element $g \in G$ is decomposable on X. Write $g = g_1 g_2$ where the g_i are disjoint on X (and each nontrivial). Let S be the socle of G.

We induct on $|X|$. Let $Y = \{X_1, \ldots, X_t\}$ be a nontrivial G-invariant partition of X with G primitive on Y. Let K be the normal subgroup of G acting trivially on Y. If $K = 1$, then G is faithful and primitive on Y, whence $G = \mathrm{Alt}(Y)$ or $\mathrm{Sym}(Y)$. Otherwise $S \leq K$ (since it is the unique minimal normal subgroup of subgroup of G containing S).

Assume that g_2 is not in K. Choose notation so that $X_1, \ldots, X_s$ with $s > 1$ is an orbit for g_2 and set $X' = X_1 \cup \ldots \cup X_s$. Then g_2 is fixed point free on this set and so g_1 must be trivial on this set. Since S leaves X'-invariant, it follows that the stabilizer of X' acts faithfully on X', a contradiction.

So we may assume that g_1 and g_2 are both trivial on Y, whence they both act on X_1 and as above both act nontrivially on X_1. So by induction, the result follows. □

Note that the previous result actually gives more information with a little more effort—when G is an alternating or symmetric group, essentially the only maximal subgroup containing H is unique and is the stabilizer of a point in the natural permutation representation (being slightly careful when $m = 6$).

Combining the results on almost simple groups allows us to state a more precise version of Theorem 2.10. Note that in the proof of that theorem, we saw that the only decomposable elements were contained in a component L of G and in particular, the component would have to be a simple group that admits an action with decomposable elements. Indeed, it follows by [2] that this action corresponds to a primitive action of $N_G(L)/C_G(L)$ and so by the result on almost simple groups $L = A_d$.

Thus we have the following result that will be useful in the final section.

Theorem 2.17. *Let G be a primitive subgroup of S_n. One of the following holds:*

(1) *Every element of G is indecomposable;*
(2) *$G = A_n, n > 5$ or $S_n, n > 3$;*
(3) *$n = d^t$ with $d \geq 5$ and $t \geq 2$, $G \leq S_d \wr S_t$ and G contains ${A_d}^t$;*
(4) *$n = 2^a, a > 2$, G contains a regular normal elementary abelian subgroup N and $G = NH$ where H is a point stabilizer and H is an irreducible subgroup of* $\mathrm{Aut}(N)$ *containing transvections.*

3. Permutation Polytopes

Now let G be any finite group, and let $\nu\colon G \to \mathrm{GL}(\mathbb{R}^n)$ be a real representation. The *representation polytope* associated with ν is the convex hull of the image of ν, a subset of $\mathrm{End}_{\mathbb{R}}(\mathbb{R}^n) \approx \mathbb{R}^{n^2}$:

$$P(\nu) := \mathrm{conv}\{\nu(g) \in \mathbb{R}^{n^2} \mid g \in G\}.$$

For each $g \in G$, left multiplication by $\nu(g)$ defines a linear automorphism of $\mathbb{R}^{n^2}$ sending $P(\nu)$ to itself and sending the image of the identity element of G to $\nu(g)$. Hence, the vertices of $P(\nu)$ are precisely the images of elements of G.

If G a subgroup of the symmetric group, S_n, we write $P(G)$ for $P(\nu_G)$ where ν_G is the natural representation of G as a group of $n \times n$ permutation matrices. In this case, we also identify each $g \in G$ with its image, $\nu(g) \in \mathbb{R}^{n^2}$. The polytope, $P(G)$, is called the *permutation polytope* associated with the permutation group G.

In this part of the paper, we establish two main results. First, we show that as G varies over subgroups of S_n, the corresponding polytope has maximal dimension $(n-1)^2$ exactly when G is 2-transitive. Next, we characterize some faces of $P(G)$ and give a bound on the diameter of the edge graph of $P(G)$.

3.1. **Dimension.** We use the following standard theorem from representation theory:

Theorem 3.1 (Frobenius and Schur [12], §27.8)**.** *Let G be a finite group, K an algebraically closed field, and $\rho_i\colon G \to \mathrm{GL}(K^{n_i})$ for $i = 1, \ldots, k$ a collection of pairwise non-isomorphic irreducible matrix representations of G. Let $x_{ij}^{(r)}$ denote the coordinate functions of ρ_r for each r. Then the set $\{x_{ij}^{(r)}\}_{i,j,r}$ of all coordinate functions is linearly independent over K.*

Let $\nu = \oplus \nu_i^{a_i}$ be the irreducible decomposition of ν over the complex numbers.

Theorem 3.2. *The dimension of the representation polytope $P(\nu)$ is*

$$\dim P(\nu) = \sum_{\nu_i \neq 1} (\deg \nu_i)^2,$$

the sum taken over all non-trivial components ν_i, not counting multiplicities.

Proof. Let $\mathbb{C}[G]$ denote the group algebra, and let ν_i be a representation of G on a complex vector space V_i for each i. There is a natural algebra homomorphism

$$\Gamma_\nu\colon \mathbb{C}[G] \to \oplus_i \mathrm{End}_{\mathbb{C}}(V_i)^{a_i} \subset \mathrm{End}_{\mathbb{C}}(\mathbb{C}^n)$$

determined by $g \mapsto \nu(g)$ for each $g \in G$ and extending linearly. The mapping Γ_ν further factors through the inclusion

$$\begin{array}{rcl} \oplus_i \mathrm{End}_{\mathbb{C}}(V_i) & \to & \oplus_i \mathrm{End}_{\mathbb{C}}(V_i)^{a_i} \\ \oplus_i \phi_i & \mapsto & \oplus_i \phi_i^{a_i} \end{array}$$

where $\phi \in \mathrm{End}_{\mathbb{C}}(V_i)$ for each i. The resulting mapping of $\mathbb{C}[G]$ into $\oplus_{i=1}^{k} \mathrm{End}(V_i)$ is a surjection by Theorem 3.1.

Restricting Γ_ν to $\mathbb{R}[G]$, the polytope $P(\nu)$ is the convex hull of the image of G. Hence, the dimension of $P(\nu)$ will be the dimension of the image of Γ_ν if the polytope contains the zero vector in its affine span and will be one less, otherwise. So it suffices to show that $P(\nu)$ does not contain $\vec{0}$ in its affine span, $\operatorname{aff}(P(\nu))$, if and only if ν contains the trivial representation as an irreducible factor. First, suppose $\vec{0} \notin \operatorname{aff}(P(\nu))$. The vector $\frac{1}{|G|}\sum_{g\in G}\nu(g)$ is an element of $P(\nu)$, hence nonzero, and its linear span is clearly G-invariant; thus, ν contains the trivial representation. Conversely, suppose that ν contains the trivial representation. Then there exists a nonzero $w \in \mathbb{C}^n$ such that $\nu(g)(w) = w$ for all $g \in G$. Given an arbitrary element $x = \sum_{g\in G} a_g\nu(g)$ in $\operatorname{aff}(P(\nu))$, we have $x(w) = (\sum a_g)w = w$, hence, $x \neq \vec{0}$, as required. □

Corollary 3.3. *If ν is a faithful representation, $P(\nu)$ is a simplex if and only if each irreducible representation of G appears up to isomorphism as a component in the irreducible decomposition of ν.*

Proof. Let $\nu = \oplus\nu_i^{a_i}$ be the irreducible decomposition of ν over $\mathbb{C}$. The polytope $P(\nu)$ is a simplex if and only if its dimension is one less then the number of vertices. In light of Theorem 3.2, the condition is equivalent to $|G| - 1 = \sum_{\nu_i\neq 1}(\deg\nu_i)^2$. However, a basic theorem of representation theory says that $|G| = \sum_\tau(\dim\tau)^2$ where the sum is over a full set of representatives of the isomorphism classes of irreducible representations of G (including the trivial representation). □

If ν is not faithful, let $H = \{g \in G \mid \nu(g) = 1\}$. In this case, $P(\nu)$ is a simplex if and only if the irreducible decomposition of ν over $\mathbb{C}$ contains each irreducible representation of G trivial on H.

Corollary 3.4. *Let $G \leq S_n$ be a subgroup having t orbits.*

(1) $\dim P(G) \leq (n-t)^2$ *with equality if and only if ν_G has at most one non-trivial factor in its irreducible decomposition;*
(2) $\dim P(G) \leq (n-1)^2$ *with equality if and only if G is 2-transitive.*
(3) *The dimension of the Birkhoff polytope, B_n, is $(n-1)^2$ for all $n \geq 1$.*
(4) *The dimension of the polytope of even permutation matrices, A_n, is $(n-1)^2$ for $n \geq 4$.*

Proof. Consider the irreducible decomposition of the permutation representation $\nu_G = \oplus_i\nu_i^{a_i}$ over $\mathbb{C}$. It is well-known from representation theory that the number of copies of the trivial representation appearing in ν is the number of orbits, t ([12] §32.3). Let $\nu_1, \ldots, \nu_k$ be the nontrivial factors of ν_G. Then $\sum_{i=1}^k \deg\nu_i = n - t$ and by Theorem 3.2, the dimension of $P(G) = \sum_{\nu_i\neq 1}(\deg\nu_i)^2$. The sum is maximized when $k \leq 1$. This proves part 1.

For part 2, by standard representation theory of permutation groups, G is 2-transitive if and only if $\nu_G = 1 + \tilde{\nu}_G$ for some irreducible $\tilde{\nu}_G$ ([12] §32.5). Parts 3 and 4 then follow since the relevant groups are 2-transitive. □

3.2. **Faces.** Let $G \leq S_n$ be a permutation group, and identify elements of G with $n \times n$ permutation matrices as usual. For $g, h \in G$, write $h \preceq g$ if the set of cycles of h is a subset of the set of cycles of g (so $M(h) \cap M(h^{-1}g)$ is empty). The element g is indecomposable when $h \preceq g$ always implies h is the identity or g.

Theorem 3.5. *The smallest face of $P(G)$ containing $g, h \in G$ is*

$$F_{\{g,h\}} := \operatorname{conv}\{hk \in G \mid k \preceq h^{-1}g\}.$$

In particular, there is an edge connecting g and h if and only if $h^{-1}g$ is indecomposable.

Proof. By symmetry, we may assume that h is the identity, e, and show that the smallest face containing g and e is $\operatorname{conv}\{k \in G \mid k \preceq g\}$. If $k \preceq g$, let $k' = k^{-1}g$. From $g = kk'$ with $k, k' \preceq g$, it follows that

$$e + g = k + k'. \tag{1}$$

Let $c \in \mathbb{R}^{n^2}$ and $b \in \mathbb{R}$ with Euclidean inner products $\langle c, g\rangle = \langle c, e\rangle = b$ and $\langle c, f\rangle \leq b$ for all $f \in G$; so c defines a face of $P(G)$ containing g and e. Equation 1 then implies that $\langle c, k\rangle = \langle c, k'\rangle = b$, too. Hence, any face containing g and e must also contain k and k'.

For any matrix $m \in \mathbb{R}^{n^2}$, define the *support* of m by

$$\operatorname{supp}(m) = \{(i,j) \in \{1, \ldots, n\}^2 \mid m_{ij} \neq 0\}.$$

Define the matrix $c \in \mathbb{R}^{n^2}$ by

$$c_{ij} = \begin{cases} 1 & \text{if } (i,j) \in \operatorname{supp}(g+e), \\ 0 & \text{otherwise.} \end{cases}$$

It follows that $\langle c, g\rangle = \langle c, e\rangle = n$ and for any $f \in G$,

$$\langle c, f\rangle = \sum_{(i,j)\in \operatorname{supp(g+e)}} f_{ij} \leq n$$

with equality if and only if $f \preceq g$. Hence, c defines a face—the smallest face, $F_{\{g,e\}}$—containing both g and e. □

Note that if $g = g_1 \ldots g_t$ with $g, g_1 \cdots, g_t \in G$ and such that the cycles of $g_1, \ldots, g_t$ are disjoint, then

$$g - e = \sum_{i=1}^{t} (g_i - e),$$

hence, g is affinely dependent on $g_1, \ldots, g_t$.

A direct computation based on the theorem establishes the following known results [4], [25], [11]:

Corollary 3.6.

(1) *The diameter of* $P(S_n)$ *is* 1 *for* $n < 4$ *and is* 2 *for* $n \geq 4$.
(2) *The diameter of* $P(A_n)$ *is* 1 *for* $n < 6$ *and is* 2 *for* $n \geq 6$.

Corollaries 2.4 and 2.5 translate into bounds on the diameter of a permutation polytope.

Corollary 3.7. *Let* $G \leq S_n$. *The diameter of the polytope* $P(G)$ *is at most* $\min\{2t, \lfloor n/2 \rfloor\}$, *where* t *is the number of nontrivial orbits of* G. *In particular, if* G *is transitive, the diameter of* $P(G)$ *is at most* 2.

The bound is sharp. For example, take G to be the direct product of t copies of the dihedral group on 4 elements, naturally considered as a subgroup of S_{4t}.

4. Mixing Times

In this section, we consider random walks on permutation polytopes or equivalently on the Cayley graph of the permutation group G with the corresponding generating set consisting of the indecomposable elements of G. This problem was suggested to us by Pak. The question about the mixing time of random walks on 0-1 polytopes goes back some time. See the survey article [26].

We generalize his result here. First we recall some notation. (see [22]).

Let G be a finite group and S a symmetric generating set for G (i.e. $G = \langle S \rangle$ and $S = S^{-1}$). Let $Q^k(g)$ be the probability that a random product of k elements of S is equal to g. Similarly, define $Q^k(A)$ to be the probability that a random product of k elements of S is in the subset A of G. Let U denote the uniform distribution on G. Define the total variation distance,

$$d(k) := (1/2) \sum_{g \in G} |Q^k(g) - 1/|G|| = \max_{A \subseteq G} |Q^k(A) - U(A)|.$$

So $d(k)$ measures how far the probability distribution Q^k is from the uniform distribution on G.

We now consider the case that G is a subgroup of S_n and S is the set of indecomposable elements in G. Clearly, S is symmetric, $1 \in S$ and $G = \langle S \rangle$. We note that $Q^k \to U$ as $k \to \infty$ (i.e. $d(k) \to 0$; this is standard since $S = S^{-1}$ and the Cayley graph is not bipartite – see for example [1]).

Theorem 4.1. *Assume that G is primitive of degree n. If G does not contain A_n, then $d(1) \to 0$ as $n \to \infty$. In all cases, $d(2) \to 0$ as $n \to \infty$.*

Pak [22] proves this for the special case $G = S_n$. The proof of this theorem follows easily from §2.3 and Pak's result. Namely, by Theorem 2.17 one of the following holds:

(1) $G = A_n$ or S_n;
(2) $n = 2^a$, G contains a regular normal subgroup N (elementary abelian of order 2^a) and a point stabilizer $H \leq \mathrm{Aut}(N)$ contains transvections and acts irreducibly on N;
(3) $n = d^t$ with $d \geq 5$, $t \geq 2$, G has a unique minimal normal subgroup $N = L \times \ldots \times L$ where $L \cong A_d$ and all decomposable elements of G are contained in one of the t minimal normal subgroups of N; or
(4) Every element of G is indecomposable.

First note, that if $d(1) \to 0$, it follows easily that $d(2) \to 0$.

In the first case, Pak [22] proved the result for S_n. A trivial modification of his proof shows that the result also holds for A_n. As Pak points out, his proof used a well-known but unpublished result of Lulov about the sum of the inverses of the degrees of the irreducible representations of the symmetric groups. A stronger version of this theorem is in Corollary 2.7 of [18].

Set $Y := G \setminus S$. So we only need prove that $|Y|/|G| \to 0$ as $n \to \infty$ in cases 2,3 and 4.

In the fourth case, Y is empty.

Consider the second case.

In the second case, the only decomposable elements are fixed point free involutions (for they must be the product of two elements each moving precisely 1/2 the points and moving no common points). Let T be the set of involutions in G which have a fixed point and induce a transvection on N. Note that if $x \in T$, then $|xN \cap T| = 2$ (indeed, $xN \cap T = x[x, N]$ and since x acts as a transvection on N, $|[x, N]| = 2$).

The list of possible H was determined by McLaughlin [19]. It follows easily from this that

$$\lim_{a \to \infty} |T \cap H|/|G|^{1/2} = 0.$$

Thus, $|Y| \leq 4|T \cap H|^2$ and so $\lim_{a\to\infty} |Y|/|G| \to 0$ as required.

Finally, consider the third case. As we saw, the only decomposable elements are in one of the t normal subgroups of N. Thus, $|Y| \leq t(d!)$ and $|G| \geq (d!)^t$. Since $t > 1$, $|Y|/|G| \to 0$ as either d or t increases.

This completes the proof of the theorem.

We now give two examples to show that if G is not primitive, the previous theorem need not hold. More precisely, we produce a sequence of groups G_p for p an odd prime such that for fixed k, $d(k)$ is bounded away from 0. In the first sequence, the Cayley graph is close to bipartite and in the second sequence, Q^1 is very small outside a proper normal subgroup.

Let $n = 2p$. Let x and y be p-cycles in S_n that are disjoint. Let u be an involution in S_n with $uxu = y$. Set $G_p = \langle x, y, u\rangle$. So $|G| = 2p^2$ and has a normal elementary abelian subgroup $N := \langle x, y\rangle$. So G is a transitive subgroup of S_n. Let S be the set of indecomposable elements in G.

Note that $xN \subset S$ and $N \cap S = \{x^i, y^i | i = 0, 1, \dots p-1\}$. So $|S \cap N| = 2p - 1$. Thus, the probability that a random element of S is in N is $(2p-1)/(p^2 + 2p - 1) < 2/p$. In particular, we see that $Q^k(N) > (1-2/p)^k$ if k is even and $Q^k(xN) > (1-2/p)^k$ if k is odd. This shows that $d(k) \to 1/2$ as $p \to \infty$. In particular, the mixing time is unbounded. Indeed, in the example, we see that the mixing time is linear in p.

Pak [22] did show that this could happen for some $0, 1$ polytopes—his example is essentially $\mathbb{Z}/2 \times S_n$.

We give another example that is similar in flavor to Pak's example. Let J be a nonabelian group of order qr with $q > r$ primes (so $r(q-1)$). Note that D embeds in S_q. Let p be a third distinct prime and consider $G = \mathbb{Z}/p \wr J$ acting on $n := pq$. Let N be the normal subgroup of G of index r. Note that the number of indecomposable elements in N is $(q-1)p^q + q(p-1) + 1$ while the number of indecomposable elements outside N is $(r-1)p^{q-1}$. So the probability that a random indecomposable element is not in N is less than $1/p$. Thus, the probability that a random product of k indecomposable elements is in N is at least $(1-1/p)^k$. So for p large compared to k, Q^k is far from uniform. Again, we see that the mixing time is linear in p.

References

[1] D. Aldous and J. Fill. Reversible Markov Chains and Random Walks on Graphs. preprint.

[2] M. Aschbacher and L. Scott. Maximal subgroups of finite groups. *J. Algebra*, 92(1):44–80, 1985.

[3] L. Babai, G. Hetyei, W. M. Kantor, A. Lubotzky, and Á. Seress. On the diameter of finite groups. In *31st Annual Symposium on Foundations of Computer Science, Vol. I, II (St. Louis, MO, 1990)*, pages 857–865. IEEE Comput. Soc. Press, Los Alamitos, CA, 1990.

[4] M. L. Balinski and Andrew Russakoff. On the assignment polytope. *SIAM Rev.*, 16:516–525, 1974.

[5] A. I. Barvinok. Combinatorial complexity of orbits in representations of the symmetric group. In *Representation theory and dynamical systems*, volume 9 of *Adv. Soviet Math.*, pages 161–182. Amer. Math. Soc., Providence, RI, 1992.

[6] A. I. Barvinok and A. M. Vershik. Methods of representations theory in combinatorial optimization problems. *Izv. Akad. Nauk SSSR Tekhn. Kibernet.*, (6):64–71, 205, 1988.

[7] Matthias Beck and Dennis Pixton. The Ehrhart polynomial of the Birkhoff polytope. *Discrete Comput. Geom.*, 30(4):623–637, 2003.

[8] Louis J. Billera and A. Sarangarajan. The combinatorics of permutation polytopes. In *Formal power series and algebraic combinatorics (New Brunswick, NJ, 1994)*, volume 24 of *DIMACS Ser. Discrete Math. Theoret. Comput. Sci.*, pages 1–23. Amer. Math. Soc., Providence, RI, 1996.

[9] Garrett Birkhoff. Three observations on linear algebra. *Univ. Nac. Tucumán. Revista A.*, 5:147–151, 1946.

[10] Richard A. Brualdi and Peter M. Gibson. Convex polyhedra of doubly stochastic matrices. I. Applications of the permanent function. *J. Combinatorial Theory Ser. A*, 22(2):194–230, 1977.

[11] Richard A. Brualdi and Bo Lian Liu. The polytope of even doubly stochastic matrices. *J. Combin. Theory Ser. A*, 57(2):243–253, 1991.

[12] Charles W. Curtis and Irving Reiner. *Representation theory of finite groups and associative algebras.* Pure and Applied Mathematics, Vol. XI. Interscience Publishers, a division of John Wiley & Sons, New York-London, 1962.

[13] Graham Ellis. Computing group resolutions. *J. Symbolic Comput.*, 38(3):1077–1118, 2004.

[14] The GAP Group. *GAP – Groups, Algorithms, and Programming, Version 4.4*, 2004. GAP homepage: `http://www.gap-system.org`.

[15] Ewgenij Gawrilow and Michael Joswig. Polymake: a framework for analyzing convex polytopes. In Gil Kalai and Günter M. Ziegler, editors, *Polytopes — Combinatorics and Computation*, pages 43–74. Birkhäuser, 2000. Homepage for Polymake: `http://www.math.tu-berlin.de/polymake/`.

[16] Robert Guralnick and Kay Magaard. On the minimal degree of a primitive permutation group. *J. Algebra*, 207(1):127–145, 1998.

[17] S. Lakshmivarahan, Jung Sing Jwo, and S. K. Dhall. Symmetry in interconnection networks based on Cayley graphs of permutation groups: a survey. *Parallel Comput.*, 19(4):361–407, 1993.

[18] M. Liebeck and A. Shalev. Fuchsian groups, coverings of Riemann surfaces, subgroup growth, random quotients and random walks. *J. Algebra*, 276 :552–601, 2004.

[19] J. McLaughlin. Some subgroups of $\mathrm{SL}_n(\mathbf{F}_2)$. *Illinois J. Math.*, 13:108–115, 1969.

[20] Shmuel Onn. Geometry, complexity, and combinatorics of permutation polytopes. *J. Combin. Theory Ser. A*, 64(1):31–49, 1993.

[21] Manfred W. Padberg and M. R. Rao. The travelling salesman problem and a class of polyhedra of diameter two. *Math. Programming*, 7:32–45, 1974.

[22] Igor Pak. Four questions on Birkhoff polytope. *Ann. Comb.*, 4(1):83–90, 2000.

[23] Gottfried Tinhofer. Cayley graphs in computer science. Notes for minicourse given at ALCCAL'2000 meeting in Varna, 2000. `http://www-m9.ma.tum.de/algograph/homepages/tinhofer/`.

[24] V. A. Yemelichev, M. M. Kovalëv, and M. K. Kravtsov. *Polytopes, graphs and optimisation*. Cambridge University Press, Cambridge, 1984. Translated from the Russian by G. H. Lawden.

[25] H. P. Young. On permutations and permutation polytopes. *Math. Programming Stud.*, (8):128–140, 1978. Polyhedral combinatorics.

[26] G. M. Ziegler. *Lectures on* 0/1*-polytopes.*, Polytopes—combinatorics and computation (Oberwolfach, 1997), 1–41, DMV Sem., 29, Birkhser, Basel, 2000.

Robert M. Guralnick, Department of Mathematics, University of Southern California, 3620 S. Vermont Ave., Los Angeles CA 90089-2532

E-mail address: guralnic@usc.edu

David Perkinson, Department of Mathematics, Reed College, Portland, OR 97202

E-mail address: davidp@reed.edu